NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

FROM RECONNAISSANCE TO SURVEILLANCE:

INTELLIGENCE TRANSFORMATION IN THE NEW MILLENNIUM

Mr. ERIC L. DAHLSTROM, DIA
COURSE 5605
DOING MILITARY STRATEGY
SEMINAR C

INSTRUCTOR
COLONEL DANIEL CUSHING, USMC

ADVISOR
MR. THEODORE M. LAVEN

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
From Reconnaissance to Surveillance: Intelligence Transformation in the New Millennium	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National War College,300 5th Avenue,Fort Lesley J. McNair,Washington,DC,20319-6000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**12**	

FROM RECONNAISSANCE TO SURVEILLANCE:

INTELLIGENCE TRANSFORMATION IN THE NEW MILLENNIUM

> The Information Revolution is not just about cheaper communications or faster computers. The Information Revolution is also changing how people *use* information. As a result, organizations such as the intelligence community must change their modi operandi in order to provide it. The Information Revolution is bringing into question many of the basic principles about how intelligence is "supposed to work." To adapt, the intelligence community must abandon many of these principles replacing them with a new approach.[1]
>
> -- Bruce Berkowitz

The vehicle moved steadily along a dusty road 175 kilometers east of the capital city of Sana'a.[2] The American pilot received permission to engage and, peering at his video screen, centered the crosshairs of his Hellfire missile directly over the target. A few moments later, the sedan carrying six al-Qaeda terrorists dissolved into a mass of fire and debris. What makes this mission unique compared to the thousands of others flown during Operation ENDURING FREEDOM is that this pilot is not a military officer. In fact, the CIA pilot is not even aboard his aircraft, a 1,500-pound Predator drone. He is "flying" this mission from a command trailer located hundreds of miles from the battlefield.[3] This one event represents a major turning point in America's military evolution. It highlights the changing nature of the threat to the United

---

[1] Bruce D. Berkowitz and Allan E. Goodman, Best Truth: Intelligence in the Information Age (New Haven: Yale University Press, 2000), ix.

[2] Mark Huband and Mark O'Dell, "Unmanned Weapon Makes its Mark in Yemeni Sea of Sand: The Predator that hit al-Qaeda Men Hiding in Desert Opened a New Front in the Global War on Terror," The Financial Times Limited, 6 November 2002, 24. Lexis-Nexis (14 April 2003)

[3] Keay Davidson, "Predator Drones are the Future of Warfare," The San Francisco Chronicle, 6 November 2002, A15. Lexis-Nexis (14 April 2003)

States and showcases the emerging capabilities required to successfully defend our country in the new millennium.

Transnational terrorist groups, willing to conduct suicide missions and eager to obtain weapons of mass destruction, pose a difficult problem for militaries geared to combat conventional foes. Because groups such as al-Qaeda operate in the midst of civilian populations and strike non-military targets, it is nearly impossible to defend the homeland without drastically changing our way of life. As such, the new National Security Strategy proposes that the United States not wait to be attacked, but should preempt terrorist groups before they can strike.[4] The American military will need specific and timely intelligence if it is going to take the fight to the terrorists. The intelligence community, in turn, must significantly change the way it processes information and move from a collection paradigm dominated by reconnaissance to one geared toward persistent surveillance on demand.[5]

New Enemies Require New Methods

Intelligence analysts start with a meager evidentiary base and strive to complete the geopolitical mosaic with limited collection information. For hundreds of years, the primary means for doing this was reconnaissance. Military decisionmakers relied on spies, cavalry, aircraft, and sophisticated satellites to provide periodic information on the activities and resources of an enemy or potential foe.[6]

---

[4] The National Security Strategy of the United States of America, (Washington, D.C.: GPO, 2002), 6.

[5] For the purposes of this paper, reconnaissance is defined as a mission undertaken to obtain, by visual observation or other detection methods, periodic information about the activities and resources of an enemy or potential enemy. Surveillance refers to the continual observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means.

[6] James O. Norman, "The Rise of Surveillance" (Master's Thesis, Air War College, Alabama, 2001), 10.

Reconnaissance proved to be extremely valuable, especially when applied against a conventional military threat. Periodic glimpses of enemy garrisons, airfields, or ports can determine the size and disposition of most military forces. Analysts merge this data with political and economic assessments to determine the capabilities and probable intentions of the enemy. The value of reconnaissance diminishes, however, when the threat shifts from a conventional military force to an unconventional group such as al-Qaeda.[7] Terrorists have no airfields or ports to monitor. Aside from the occasional training camp, al-Qaeda terrorists live and operate within the civilian state infrastructure.

Today's transnational terrorist groups pose a unique threat. They operate in the shadows like underground criminal organizations; yet have the potential to inflict an enormous number of casualties.[8] Due to the terrorist's clandestine nature, the intelligence community cannot rely solely upon reconnaissance for collecting information against these groups. Today's collectors must incorporate the same techniques that law enforcement organizations used to dismantle mafia syndicates in New York and drug cartels in South America. Police forces use informants and reconnaissance to focus their search for potential criminals. But once suspects are identified, police forces routinely employ persistent surveillance to track and monitor their activities until an arrest can be made. Without persistent surveillance, the police would be searching for a needle in a haystack—not unlike the U.S. military's hunt for Mohammed Aideed in Somalia, Osama bin Laden in Afghanistan, and Saddam Hussein in Iraq.

---

[7] Berkowitz, 115.

[8] The 11 September 2001 terrorist attacks caused more American fatalities than the Japanese attack on Pearl Harbor in 1941. The employment of weapons of mass effect, such as the use of sarin gas in the Tokyo subway by the radical Aum Shinrikyo terrorist group in 1995, is an indication of the new lethality such groups can wield.

The Benefits of Surveillance

Surveillance is critical to solving the terrorist problem and can be used in different ways depending upon the political circumstances or the desired results.[9] For instance, surveillance can be used to conduct counterterrorist strikes or merely as a means of collecting information on individuals, groups, or locations. Surveillance can also be used to compel terrorists to act or to deter them from striking the United States or our friends and allies. Applying persistent surveillance against terrorist groups eliminates the one advantage they hold over conventional forces—the ability to operate in the shadows.

The Predator strike in Yemen is a classic example of how persistent surveillance can be used to support counterterrorist operations.[10] The al-Qaeda suspects were identified via human and electronic means and immediately tracked with the optical sensors aboard the unmanned drone.[11] The decision to strike was made when the automobile carrying the terrorists reached a location where collateral damage would be avoided. Applying the same techniques that al-Qaeda used on 11 September, the CIA pilot turned the hunter into the hunted. Through the Predator's surveillance capability, Washington was able to strike at a time and place of its own choosing, without alerting the target that he was under attack.

There will also be circumstances when the United States would rather watch than act. The Israelis used surveillance drones loitering unseen and unheard above Arab neighborhoods during

---

[9] Louis Andre, interview by Eric Dahlstrom, National War College, 10 April 2003.

[10] The airstrike against Saddam Hussein and his leadership in the suburbs of Baghdad on 8 April 2003 would not be an example of persistent surveillance. The human source that reported Hussein's whereabouts broke contact and could not determine whether or not the Iraqi leader departed the restaurant prior to the bombing.

[11] Philip Smucker, "The Intrigue Behind the Drone Strike: Yemen Official Says US Lacks Discretion as Antiterror Partner," Christian Science Monitor, 12 November 2002, 1. ProQuest (31 March 2003)

Intifada uprisings on the West Bank in the 1990s.[12] The Israeli Army would then send in tanks causing the Arab fighters to flee to safe houses throughout the town. The drone monitored this activity and intelligence analysts identified the havens. After localizing these potential targets, Israeli intelligence focused clandestine human and signals intelligence collection to gain more detailed information on terrorist plans and intentions. Washington can apply similar techniques against al-Qaeda in order to identify and exploit leaders, operatives, and facilities.

Surveillance can also force terrorists to act—or not to act. People behave differently when they know they are being watched. Predator-type unmanned aerial vehicles flying low enough to be heard or seen from the ground can be a deterrent if used above suspected terrorist strongholds or potential targets. The fear of an imminent counterterrorist strike may prohibit groups from conducting attacks or force them to consider less valuable targets. Moreover, overt surveillance may compel terrorists to abandon established methods of operation and initiate new patterns of behavior. When terrorists are forced to change their plans, it makes them vulnerable to other forms of intelligence collection and military action.[13]

Developing a Surveillance Capability

Although the United States is making great strides, it has not yet reached the point where it can routinely apply persistent surveillance on demand.[14] The military has its own brand of informants (HUMINT) and the most sophisticated reconnaissance assets in the world. Used

---

[12] David A. Fulghum and Robert Wall, "Israel's Future Includes Armed, Long-Range UAVs." Aviation Week & Space Technology, 24 June 2002. ProQuest (20 April 2003)

[13] Andre, interview.

[14] This is particularly true when the target is an individual. The Joint Surveillance and Target Attack Radar (JSTARS) is very good at monitoring vehicular activity, but is not effective against human beings.

together, the United States has a tremendous capability to identify potential terrorists. What the military lacks is an integrated strategy for adequately tracking these suspects once they are identified. The Predator example discussed earlier represents only the first step in this process.

The United States is the most technologically advanced nation on earth. All-weather sensors and breakthroughs in radio frequency tagging are on the horizon and soon will be incorporated into America's intelligence collection arsenal.[15] The real challenge, however, is not developing these sensors, but in integrating them with existing collection systems and applying them to new intelligence methodologies. In the fight against global terrorism, the key is linking identification to surveillance. Once a terrorist is found, it is necessary to immediately apply surveillance (whether human or machine; optical or acoustic) to the target. This entails blending collection assets into a unified, seamless intelligence capability and employing a strategy that quickly permits intelligence to make the handoff from identification to tracking.

The Yemen example used multiple collection sensors working in concert to localize, identify, and track the al-Qaeda terrorists. The global positioning coordinates provided by the leader's cellular phone identified the town where the suspect lived.[16] Human intelligence was able to identify the individual and pinpoint his exact location and mode of transportation. Finally, the Predator's imagery allowed the CIA to track the terrorists and ultimately eliminate the threat. This example should act as a model for how to coordinate and integrate various collection disciplines into a counterterrorism strategy that uses persistent surveillance to achieve a successful outcome.

---

[15] Brian Albright, "Eye Spy," Frontline Solutions, October 2002, 16. ProQuest (21 April 2003)

[16] Smucker, 1.

Breaking the Analysis Paradigm

Despite the development of such surveillance assets as Predator, Global Hawk, and the Joint Surveillance and Target Attack Radar (JSTARS), the intelligence community has not updated its traditional way of thinking about how to process collected information.[17] Still operating under a reconnaissance mindset, the intelligence community prefers to receive its intelligence data first, then conduct the analysis to determine what the information means and how it might impact existing intelligence assessments. This is a reactive approach—and it worked well fifty years ago when there was enough time to decipher new information, assess the ramifications, and task additional collection to help define the problem.

The new terrorist threat does not allow for the time-intensive intelligence cycle to play out. When information is acquired on a terrorist suspect, the United States must act quickly to determine the nature of the threat and decide upon how best to deal with it. Once persistent surveillance is placed upon a target of interest, the United States may have only a matter of minutes, or possibly a few hours, to decide how to act in order to neutralize or eliminate the threat. If this information is passed real time to an armed aircraft, such as in the Predator example, the decision to use—or not to use—force is needed almost instantaneously.

The traditional method of performing intelligence analysis must be revamped. There will not be enough time to conduct surveillance and then analyze the data to determine if the suspect should be targeted or not. The analysis must be moved to the front of the intelligence process and conducted *before* the surveillance is applied to the suspect.[18] This requires the analyst to approach the problem in a new way. Like a police officer, the intelligence analyst must do the

---

[17] Berkowitz, 113-115.

[18] Andre, interview.

investigative legwork first—using the full range of human and electronic sources to localize and identify the suspect. Only then can surveillance be applied to track the terrorist and permit a decision to be made regarding how to prosecute the threat.

Reaching Decision Superiority

"The record is quite clear: the side that acts faster wins. This is the essence of a decision-superior force."[19] It is also the key to winning the war on global terrorism. Acting faster means, in large part, reducing the time needed to move information from sensor to shooter. The only reliable means for accomplishing this is through persistent surveillance. The warfighter must know who the enemy is and where he is at those critical times when decisions must be made or actions taken. Reconnaissance leaves gaps that create doubt as to the accuracy of the information—surveillance does not. This does not mean that surveillance has to be permanent to be effective. It only has to be available when needed; hence the requirement for persistent surveillance *on demand*.

Surveillance by its very nature provides more information than reconnaissance. The intelligence analyst can provide better assessments because he works with more evidence and less assumptions.[20] And while this contributes to more and better intelligence, it does not ensure decision superiority. Defense leaders, whether on the battlefield or in the Pentagon, must have access to accurate information in a manner that is timely and conducive for making decisions. It is only when surveillance, fused with other collection data and analysis, is integrated into a fully accessible information management system, that decision superiority can be achieved.

---

[19] Richard B. Myers, "A Word From the Chairman," Joint Forces Quarterly, Summer 2002, 7.

[20] Andre, interview.

Intelligence analysts are inundated with collection information generated by reconnaissance assets to the point where only a portion of the data is analyzed in a timely manner.[21] Despite this glut of information, the intelligence community was not successful in defending America from the al-Qaeda strikes in September 2001. To meet the emerging terrorist threat, intelligence analysts must change the way they manage this information. For a start, they must do the analysis up front to help focus the reconnaissance against high-value suspects. Once targets are localized and identified, persistent surveillance must be applied to track the terrorists until action can be taken to neutralize the threat. Only by shifting the way it does business—from the old reconnaissance paradigm to the new surveillance model—will the intelligence community and the U.S. military hope to defeat al-Qaeda and the other transnational terrorist groups that threaten our nation.

---

[21] Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington D.C.: CQ Press, 2000), 55.

BIBLIOGRAPHY

"A High-Tech Pilot Who Keeps His Feet on the Ground," The Washington Post, 7 March 2003. ProQuest (31 March 2003)

Albright, Brian, "Eye Spy," Frontline Solutions, October 2002. ProQuest (21 April 2003)

Atkins, Charles, "Intelligence Transformation: Beyond Paradigm Shifts, Changes in Ethos," Military Intelligence Professional Bulletin, Oct-Dec 2000. ProQuest (31 March 2003)

Berkowitz, Bruce, "Deep Cover," Hoover Digest, Fall 2002. <http://www.hoover.Stanford.edu/publications/digest/024/berkowitz.html> (13 April 2003)

Berkowitz, Bruce D. and Allan E. Goodman, Best Truth: Intelligence in the Information Age. New Haven: Yale University Press, 2000.

Bond, Stephen J., "Coalition Aerial Surveillance and Reconnaissance: The CAESAR Project," Military Intelligence Professional Bulletin, Jan-Mar 2003. ProQuest (31 March 2003)

Bowers, Faye, "US Pulls Out New Tools, New Rules: CIA Slaying by Drone Signals Bush's Resolve to Hunt Down Al-Qaeda, Even by Controversial Means," The Christian Science Monitor, 6 November 2002. ProQuest (31 March 2003)

Caterinicchia, Dan and Matthew French, "DOD Funnels Money into Transformation," Federal Computer Week, 10 February 2003. ProQuest (31 March 2003)

Chizek, Judy G., "Military Transformation: Intelligence, Surveillance and Reconnaissance," Report for Congress, 31 May 2002.

Covault, Craig, "Secret NRO Recon Eye Iraqi Threats," Aviation Week & Space Technology, 16 September 2002. ProQuest (31 March 2003)

Davidson, Keay, "Predator Drones are the Future of Warfare," The San Francisco Chronicle, 6 November 2002. Lexis-Nexis (14 April 2003)

"DOD To Stress Transformation in FY '04 Budget," Defense Daily, 23 January 2003. ProQuest (31 March 2003)

Fatzinger, Eric W., "Military Intelligence Transformation," Military Intelligence Professional Bulletin, Oct-Dec 2001. ProQuest (31 March 2003)

Fulghum, David A. and Robert Wall, "Israel's Future Includes Armed, Long-Range UAVs," Aviation Week & Space Technology, 24 June 2002. ProQuest (20 April 2003)

Hersh, Seymour M., "Manhunt: The Bush Administration's New Strategy in the War Against Terrorism," The New Yorker, 23 December 2002. Lexis-Nexis (14 April 2003)

Huband, Mark and Mark O'Dell, "Unmanned Weapon Makes its Mark in Yemeni Sea of Sand: The Predator that Hit al-Qaeda Men Hiding in Desert Opened a New Front in the Global War on Terror," The Financial Times Limited, 6 November 2002. Lexis-Nexis (14 April 2003)

Lewis, Paul, "Future Shocks: As Old Certainties Wither, The Shifting Sands of International Conflict are Leading the USA to Reassess its Weaponry Needs for the New Century," Flight International, 10 September 2002. Lexis-Nexis (14 April 2003)

Liddy, James G., "Capabilities, Capabilities, Capabilities," Proceedings, October 2002. ProQuest (31 March 2003)

Lowenthal, Mark M. Intelligence: From Secrets to Policy. Washington D.C.: CQ Press, 2000.

Lumpkin, John J., "U.S. Kills Senior al-Qaeda Operative in Yemen with Missile Strike," The Associated Press, 5 November 2002. Lexis-Nexis (14 April 2003)

Myers, Richard B., "A Word From the Chairman," Joint Force Quarterly, Summer 2002.

Norman, James O., "The Rise of Surveillance," Master's Thesis, Air War College, 2001.

O'Hanlon, Michael, Technological Change and the Future of Warfare. Washington D.C.: Brookings Institution Press, 2000.

"QDR Looks to Space," Aerospace America, January 2002. Lexis-Nexis (14 April 2003)

Risen, James and David Johnston, "Bush Has Widened Authority of CIA to Kill Terrorists," The New York Times, 15 December 2002. ProQuest (31 March 2003)

Smucker, Philip, "The Intrigue Behind the Drone Strike: Yemeni Official Says US Lacks Discretion as Antiterror Partner," The Christian Science Monitor, 12 November 2002. ProQuest (31 March 2003)

Taylor, Michael C., "Benchmark for Intelligence Transformation," Military Intelligence Professional Bulletin, Jan-Mar 2003. ProQuest (31 March 2003)

The National Security Strategy of the United States of America, Washington, D.C.: GPO, 2002.